Trust Evaluation Model for Mobile Ad Hoc Network

M.B. Mukesh Krishnan, Prof. Dr. P. Sheik Abdul Khader

ABSTRACT

Securing Mobile ad hoc net work is a challenging task due to the lack of trust among nodes. In this paper we analysis various trust models for Mobile ad hoc network and then propose a trust evaluation model for mobile ad hoc network which estimating trust level of supplicant nodes by Evaluating and analysis node behavior. This model also designed to detect compromised nodes inside the environment and to isolating the compromised and misbehavior nodes from the network. This model also tested through introducing misbehavior nodes and compromised nodes into the environment and the result shows that the model is highly effective in detecting misbehavior node and compromised nodes over various other security models for Mobile ad hoc network.

Keywords - MANET, Trust, Node Misbehavior, Compromised Node.

1. INTRODUCTION

Mobile ad hoc networks pose security challenges due to the autonomous nodes, inadequate physical protection that leads to nodes captured, compromised and hijacked. There higher possibility for malicious attacks launched from both outside and inside the network. It is difficult to track down a malicious node in a large scale of ad hoc network, attacks from a compromised node are more dangerous and much harder to detect. All these indicate that any node must be prepared to operate in a mode that should not immediately trust on any peer. Any security solution with static configuration would not be sufficient because of the dynamic topology of the networks. Generally, decision making in the mobile ad hoc networks is decentralized and many on the cooperation of all nodes or partial nodes. But new type of attacks can be designed to break the cooperative algorithm. Malicious nodes could simply block or modify the data traffic traversing them by refusing the cooperation or hacking the cooperation. As can be seen from the above things, the lacking in the mobile ad hoc networks is trust since each node must not trust any other node immediately. If the trust relationship among the network nodes is available for every node, it will be much easier to select proper security measure to establish the required protection. It will be wiser to avoid the un-trusted nodes as routers. Moreover, it will be more sensible to reject or ignore hostile service requests. Therefore, the trust evaluation becomes a before-security issue in the mobile ad hoc networks. The security solution should be dynamic based on the changed trust relationship.

2. TRUST MODELS IN MANET

Various trust models are proposed to MANET such as The PGP (Pretty Good Privacy) trust model proposed by Jean-Pierre Hubaux, Levente Buttyan and Srdjan Capkun [5], the design of PGP by establishing a public-key distribution system and public –key certificates are issued ,signed and verified by nodes in MANET themselves based on their individual acquaintances. But, in contrast to PGP no continuously accessible public-key directories for the distribution of public-key certificates are necessary. Ant-based trust algorithm proposed by Tao Jiang and John S. Baras, presents a scheme for distributing Trust Certificates in mobile ad-hoc networks. The core of the model is the ABED-Ant-Based Evidence Distribution Algorithm, which is fundamentally based on the Swarm Intelligence Paradigm generally used for optimization problems, for example the Traveling Salesman Problem (TSP) . The major idea of the paradigm is expressed by the term stigmergy offering a method for communications in systems by which the individual parts communicate with one another by modifying the environment and without direct interactions Using semirings to evaluate trust in MANET Theodorakopoulos G, Baras J[1][2]The concept is how to establish an indirect trust relationship without previous direct interactions within an ad-hoc network is introduced. By the use of the theory of semirings, the presented approach is also robust in the presence of attackers. The significant idea is to model the trust inference problem as a generalized shortest path problem on a weighted graph G(V,E), also referred to as the trust graph. A weighted edge corresponds to the opinion, consisting of two values the trust value and the confidence value that an entity has about another entity in the graph (network).

3. TRUST EVALUATION MODEL FOR MOBILE AD HOC NETWORK

In this session we discuss about the trust evaluation model for mobile ad hoc network. During the cluster formation in MANET cluster head sends one or more authentication request packets to the adjacent node with the one – time password along with that. There are two possible scenario can occur at this stage.

Scenario1: Using the one – time password node can join the cluster/group

Scenario2: The node which received the one – time password broadcast the password to other nodes.

Once the scenario2 can be possible we should be careful because all the nodes in the environment are not trusted nodes .The last session enlisted the various trust models in MANET to resolve this kind of problem but main area where all models concentrated but still remain as open problem are listed as follows

- Policy to disclosing of privacy information
- Policy to authenticate the nodes
- Access a node as intermediate during communication
- Resource sharing between supplier and supplicant.
- Trust chain formation between nodes
- In this paper we propose a Trust evaluation model for Mobile Ad Hoc Network which address the above mentioned problem through two sub process
- Supplicant node Trust estimation.
- Group privacy agreement

3.1 Supplicant Node Trust Estimation

The core aim of supplicant node trust estimation is done through evaluating and analysis node behavior. Before the node enables communication cluster formation will be done at the time cluster head will supply one time authentication password to enable the other nodes to identify the node and that password is updated in cluster database which can't by all nodes only cluster head access them. We also maintain another database called network information database in which the network log are stored. This process starts when supplicant ask the supplier node to supply.

Step 1 : Send request for supplicant nodes traffic information.

Step 2 : Collect node traffic information of adjacent node through cluster network information database.

Step 3 : Ask for certificate to ensure the node belongs to the cluster

Step 4 : Evaluate the certificate authentication and traffic information

Step 5 : Ask for supplicant node sequence information

Step 6 : Ask for One time authentication password generated and issued by cluster head during cluster formation.

Step 7 : Send the authentication password to cluster head for verification

Step 8 : If

verification success cluster head send the success message and send a new one time password to the adjacent node

Else

Sends an unsuccessful message.

Step 9 : If

Evaluation and Analysis result will not find any compromised behavior of the node and verification message is success then adjacent node trust is established

Else

Isolate the adjacent node from the network

Fig1. Supplicant node Trust estimation.

3.2. Group Policy Agreement

The group policy agreement is established to detect and discard the compromised nodes. The process will follow the following methodology. If the supplicant node trust estimation is positive and supplier accepts for communication, a group policy agreement is made between the supplier and supplicant to retain the trust until the service ends between them. As a part of agreement supplicant will not access or communicate to any other node during the communication. It is ensured by locking all the ports in the supplicant node except the port for communication with the supplier it enables the communication secured. Along with this if the supplicant node report more than three failure transition then the supplicant is send to supplicant node trust estimation phase and come back to group policy agreement. If the supplicant node accepts the policy the supplier and supplicant group policy agreement is imposed and communication established else the supplicant is discarded.

4. STIMULATION AND PERFORMANCE ANALYSIS

In this section we present the stimulation setup and performance analysis. We create 10% of the nodes inside the network as malicious nodes and it creates the 20% of node as malicious node through the compromised behavior of the node. We also consider all malicious nodes are capable of creating compromised nodes. NS/2version 2.34 software is used for the model implementation. The simulations were based on 1000 by 1000 flat space scattered with 100 wireless nodes. The nodes move through the radio – propagation from a random starting point to a destination with a speed ranging from 0-20 m/sec as the destination is reached another destination be targeted after a pause time of 5sec. The MAC layer used for simulations is IEEE 802.11. The Intrusion detection system and

authentication key model are incorporated. Traffic sources and the attacks are given as a source input with each data packet of 512 bytes long. all nodes in the network were made the sources and the destinations were spread randomly across the network. The mobility model used is random walk. Duration of the simulations is 900 seconds. Separate simulations were performed for the malicious node created in the network and after the implementation of the trust estimation model.

In this part we describe the stimulation scenarios and analysis the performance. The stimulation was through two scenarios.

In the first scenario supplicant is malicious node which falls under the 10% which we created.

In the second scenario supplicant is compromised node due to the attacks which falls under 20% of the compromised node created by the malicious nodes.

Through this scenario we calculated the malicious node and compromised node detection and false positive detections and the result showed that this model detection is 72% and false positive detection is 21%. Similarly we also injected the same type attacks to various trust model and the result shows that detection percentage ranges between 47% to 61% and the false positive detection ranges between 22% to 46%, it shows that trust estimation model for mobile ad hoc network detects malicious and compromised node better than other models.

5. CONCLUSION

The trust estimation model for MANET which provided the trust through supplicant node Trust estimation and group privacy agreement is also tested using ns/2 and the result shows that the model performs between than the other models proposed for establish trust in MANET.

6. REFERENCES

1. Jiang T, Baras J (2004) Ant-based Adaptive Trust Evidence Distribution in MANET. In: 2nd International Workshop on Mobile Distributed Computing. USA: pp 588–593
2. Jiang T, Baras J (2004) Cooperative Games, Phase Transition on Graphs and Distributed Trust MANET. In: 43rd IEEE Conference on Decision and Control
3. Theodorakopoulos G, Baras J (2004) Trust Evaluation in Ad-Hoc Networks. In: ACM workshop on Wireless security. USA: pp1–10
4. Zimmermann PR (1995) The Official PGP User's Guide. MIT Press USA

5. Hubaux JP, Buttyan L, Capkun S (2001) The Quest for Security in Mobile AdHoc Networks. In: 2nd ACM international symposium on Mobile ad hoc networking & computing. USA: pp 146–155
6. M. E. G. Moe, B. E. Helvik, and S. J. Knapskog, "TSR: Trust-basedSecure MANET Routing using HMMs," Proc. 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Vancouver,British Columbia, Canada, 27-28 Oct. 2008, pp. 83-90.
7. S. Reidt, S. D. Wolthusen, and S. Balfe, "Robust and EfficientCommunication Overlays for Trust Authority Computations," Proc. 2009 IEEE Sarnoff Symposium, March 2009.
8. M. A. Ayachi, C. Bidan, T. Abbes, and A. Bouhoula, "MisbehaviorDetection Using Implicit Trust Relations in the AODV Routing Protocol," 2009 Int'l Conf. on Computational Science and Engineering, Vancouver, Canada, vol. 2, 29-31 Aug. 2009, pp. 802-808.
9. A. Adnane, C. Bidan, R. T. de Sousa, "Trust-based Countermeasures for Securing OLSR Protocol," 2009 Int'l Conf. on Computational Science and Engineering, Vancouver, Canada, vol. 2, 28-31 Aug. 2009,pp.745-752.

AUTHOR'S PROFILE

M.B.Mukesh Krishnan received his B.Sc in Mathematics from Presidency College , Chennai , India in 1999, his MCA degree from Periyar University, Salem, India in 2002 and his M.Tech in Information Technology from Vellore Institute of Technology, Vellore , India in 2005.Currently doing his Ph.D in Sathyabama University, Chennai , India . His research interest includes Wireless Networks , Mobile Computing , Ad hoc networks, Mobile Ad hoc Networks and Network Security.

P. Shiek Abdul Khader recived his M.Sc. in Applied Mathematics from Anna University, India, M.Phil from University of Madras, Chennai, India and Ph.D from Anna University, Chennai , India. His research includes Computer Networks, Neural Networks, Fuzzy Logic,Genetic Algorithm,System Programming, Software Engineering, Numerical Methods and Operations Research.